REMARKS

Claim 1 is pending. Claims 2-30 are canceled.

Claim 1 is rejected under 35 U.S.C. §112, second paragraph, as indefinite. Claim 1 has been amended to address this objection and is thus allowable.

Claim 1 is also rejected under 35 U.S.C. §101, as non-statutory. Claim 1 has been amended to address this objection and is thus allowable.

Finally, Claim 1 is rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 7,281,139 to Stewart ("Stewart") in view of U.S. Patent No. 6,412,009 to Erickson ("Erickson") and further in view of U.S. Patent No. 6,092,196 to Reiche ("Reiche"). Applicant respectfully traverses this rejection.

The present invention provides a method for a server to use a communications protocol that the server does not implement to obtain information from a client. In various embodiments, a primary server receives a request generated by a client. The primary server then sends a first request to a secondary server as part of processing the request generated by the client. While the secondary server is processing the first request from the primary server, it determines a need for data obtainable from a client application that supports user interaction by using a communications protocol that the secondary server is not configured to implement. The secondary server then sends a second request to the primary server for obtaining the data resulting from using the communication protocol. Subsequently, the secondary server receives the resulting data and continues to process the first request using the resulting data. Thereafter, the secondary server returns a response for the first request to the primary server.

More specifically, authentication services are often implemented to control access to Web-based applications. Such authentication services, which may be implemented as a Web server plug-in, a reverse proxy, other type of server-side component, require a user to prove their identity to an appropriate level of certainty. To perform an authentication procedure, a protocol engine in the afore-mentioned server-side component communicates directly with a client application using a protocol, such as the Hypertext Transport Protocol (HTTP). This communication with the client application often requires client-focus. In other words, some type of control of the processing flow from the client-side perspective during the authentication process, which may often include user interaction through the client application.

However, it is not uncommon for information technology (IT) professionals to have a need to further enhance their security systems. As a result, some of the afore-mentioned client-side components may be restricted from either executing or implementing certain protocols. In particular, these protocols include advanced protocols that are used by authentication services for user authentication and attribute exchange requiring communication with Web browsers or similar types of client applications. Accordingly, the present invention provides a method of enabling a server-side component that is not implemented with a particular protocol to access an implementation of the protocol within other server-side components where it is implemented.

With respect to Claim 1, Examiner asserts that Stewart discloses the limitations of Claim 1, where an FTP server is the primary server and a Web server is the secondary server (Figure 4, col. 4, lines 45-49). Applicants respectfully disagree.

The disclosure of Stewart relates to a system and method for authenticating a legacy service using Internet technology. More specifically, Stewart discloses associating an authentication module with a legacy server. Service requests from a user of the legacy server are passed to the authentication module. In turn the authentication module generates a service request for a Web server, requesting access to a protected page from the Web server and likewise transmitting the user's credentials to the Web server. The Web server attempts to access the protected legacy server, which causes the Web server to access a network-based authentication service to determine whether the user's credentials qualify for access to the previously requested protected page. The Web server transmits a message back to the authentication module, which determines from the message whether the user's credentials qualify for access to the legacy server (abstract).

The portion of the cited reference discloses that ". . . the FTP authentication module may emulate a Web browser in its communication with the Web server. The FTP authentication module may send a request to (the) Web server, specifying a URI (possibly by means of a proxy server)." Accordingly, the FTP authentication module implements the HTTP protocol to emulate a Web browser when communicating with the Web server (i.e., the secondary server), which likewise implements the HTTP protocol. In contrast, the HTTP protocol is not implemented on the secondary server in the present invention. Instead, a protocol engine in the afore-mentioned server-side component of the present invention communicates directly with a client application using a protocol, such as HTTP. Stewart further discloses ". . . the FTP server uses the Web

server as a proxy server for authentication purposes (col. 4, lines 19-20)." This is in direct contrast to the present invention where the primary server is an authentication server and the secondary server is a Web server that does not implement a client-oriented communications protocol such as HTTP. Furthermore, Stewart is silent on the implementation of a Web service on the secondary server as disclosed in the present invention. In view of the foregoing, skilled practitioners of the art would not consider the FTP server of Stewart to be equivalent to the primary server of the present invention as it emulates a client-oriented communications protocol for communicating with the Web server.

Examiner further asserts that Stewart discloses the limitation of determining a need for data (col. 4, lines 53-57). Applicants respectfully disagree.

The "need for data" disclosed in the present invention relates to determining at the secondary server a need for data that is obtainable from a client application that uses a communications protocol, such as HTTP, which is not implemented on the secondary server. More specifically, in the present invention:

> ". . . (the) secondary sever requires data that results, or is outputted from, an operation, a transaction, or other type function that is accomplished through the use of a particular communication protocol (e.g., HTTP). (The) secondary server is not configured to implement the particular communication protocol that is required for performing the operation or the type of transaction from which (the) secondary server requires data (page 16, lines 12-20).

Said using other words, the secondary server requires data that is only obtainable through the use of a communications protocol that is not implemented on the secondary server. In contrast, Stewart discloses that ". . . (the) Web server may accept the request and compare it to an access control list, determining that the requested page is protected. (the) Web server may then send a response to the FTP authentication module requesting the user's credentials (col. 4, lines 53-57)." The portion of the cited reference relates to a "need for data" by the Web server for credentials to authenticate a user. Accordingly, those of skill in the art would not consider the need for credentials by Web server of Stewart for authenticating a user to be equivalent to the need for data by the secondary server of the present invention that is obtainable from a client application using a communications protocol that is not implemented on the secondary server.

Likewise, Examiner further asserts that Stewart discloses the limitation of sending a second request (col. 4, lines 57-61). Applicants respectfully disagree.

The "sending a second request" disclosed in the present invention relates to sending a second request, comprising information for an HTTP redirect message, from the secondary server to the primary server. In contrast, the portion of the cited reference relates to the FTP authentication server of Stewart providing the Web server with the user's credentials. Furthermore, Stewart is silent on the subject of an HTTP redirect message. Accordingly, skilled practitioners of the art would not consider Stewart's disclosure of the FTP authentication server providing user credentials to a Web server to be equivalent to the present invention's disclosure of the secondary server sending a second request, comprising information for an HTTP redirect message, to the primary server.

Examiner further asserts that Stewart discloses additional limitations (col. 4, lines 57 – col. 5, line 1). Applicants respectfully disagree.

The portion of the cited reference, which is repeated here for convenience, merely describes the provision of a user's credentials to a Web server for authentication:

> The FTP authentication module may then provide the Web server with the user's credentials (which may have been previously collected by the FTP server, or may be collected in real time, e.g., by displaying a login box or form, asking the user to provide credentials). The Web Server may then authenticate the credentials against the network-based authentication service, which may determine whether the user's credentials are valid and return the user's status to web server. The status may be passed back to FTP authentication module, which determines whether to grant the user access to the FTP server based on the response from web server. If the response is positive, then access may be granted. By contrast, if the response is negative, then access may be denied.

In contrast, and as previously described herein, the present invention provides a method of enabling a server-side component that is not implemented with a particular protocol to access an implementation of the protocol within other server-side components where it is implemented, for the provision of data to the secondary server. More specifically, the data provided to the secondary server of the present invention results, or is outputted from, an operation, a transaction, or other type function that is accomplished through the use of a particular communication protocol (e.g., HTTP). The secondary server is not configured to implement the particular communication protocol that is required for performing the operation or the type of transaction from which (the) secondary server requires data (page 16, lines 12-20).

Examiner correctly states that Stewart discloses neither "the client using a HTTP protocol for which the secondary server is not configured to implement" nor an "HTTP redirect message"

as disclosed in the present invention. However, Examiner asserts that Erickson discloses the HTTP protocol limitation (Figure 1, col. 1, lines 44-61) and that it would have been obvious to use the teaching of Stewart in combination with the HTTP protocol limitation of Erickson in order to pass firewall security (col. 1, lines 44-50). Applicants respectfully disagree.

The portion of the cited reference merely describes using a Web browser to access an HTTP port to establish an intermediary Telnet session for communication with a legacy host. More specifically, Erickson discloses a Web server running a terminal emulator that provides a Telnet session with a host system. As disclosed by Erickson, the Web server receives Telnet data from the host system, and instead of displaying the data as a typical text screen, sends it to a translator. In turn, the translator translates the Telnet text into HyperText Markup Language (HTML) statements that are sent to a browser program running on a Web client. The browser then translates the HTML statements into an HTML page, which is then displayed on the Web client. Said in other words, the disclosure of Erickson teaches the implementation of a terminal emulator to emulate a communications protocol (e.g., HTTP). However, Erickson fails to disclose accessing an implementation of the protocol (e.g., HTTP) within other server-side components where it is implemented. Accordingly, those of skill in the art would consider the terminal emulator of Erickson to be equivalent to the method of the present invention for enabling a server-side component that is not implemented with a particular protocol to access an implementation of the protocol within other server-side components where it is implemented.

Examiner further asserts that Reiche discloses the limitation of an HTTP redirect message (col. 4, line 50 – col. 6, line 2) and that it would have been obvious to use the combination of Stewart and Erickson in accordance with the HTTP redirect method of Reiche to support the request even when the requested resource resides under a different Universal Resource Identifier (col. 1, lines 51-54). Applicants respectfully disagree.

The present invention discloses sending a second request, comprising information for an HTTP redirect message, from the secondary server to the primary server, for obtaining data resulting from a client using the HTTP protocol. The method disclosed by Reiche merely discloses an authentication server issuing a redirect request to a user's browser to pass a transaction ID as a parameter in a Uniform Resource Locator (URL) string (col. 5, lines 43-45). Accordingly, skilled practitioners of the art would not consider the issuance of a redirect request as disclosed by Reiche to pass a transaction ID as a parameter in a URL to be the equivalent of

sending a second request from a secondary server to a primary server for obtaining data resulting from a client using the HTTP protocol as disclosed in the present invention. Applicant respectfully submits that the combination of Stewart and Erickson in accordance with the teachings of Reiche proposed by Examiner fails to teach all the limitations recited in claim 1. In view of the foregoing, it is respectfully submitted that independent claim 1 is allowable over the art of record and the rejection under 35 U.S.C. §103(a) should be removed.

CONCLUSION

In view of the amendments and remarks set forth herein, the application is believed to be in condition for allowance and a notice to that effect is solicited. Nonetheless, should any issues remain that might be subject to resolution through a telephonic interview, the examiner is requested to telephone the undersigned at 512-338-9100. The Commissioner is authorized to deduct any fees that may be necessary and to credit any overpayment to Deposit Account 090447.

CERTIFICATE OF TRANSMISSION

I hereby certify that on July 8, 2009, this correspondence is being transmitted via the U.S. Patent & Trademark Office's electronic filing system.

/Gary W. Hamilton/

Respectfully submitted,

/Gary W. Hamilton/

Gary W. Hamilton
Attorney for Applicant(s)
Reg. No. 31,834